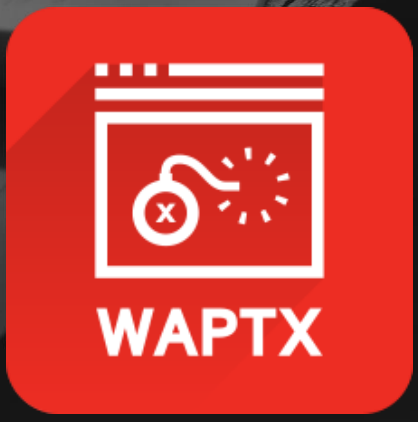
SYLLABUS



WEB APPLICATION PENETRATION TESTING EXTREME

VERSION 2

The most advanced course on web application penetration testing

eLearn Security
AN INE COMPANY

eLearnSecurity has been chosen by students in 140 countries in the world and by leading organizations such as:

hp Microsoft intel cisco AT&T verizon U.S. AIR FORCE pwc gemalto

COURSE DESCRIPTION

Web Application Penetration Testing eXtreme is a practical online course on the most advanced web application penetration testing techniques.

This training course is tied to Hera Lab, where students will access a number of laboratories for each learning module.

PRE-REQUISITES

WAPTX is an advanced course that requires the following pre-requisites:

- Deep understanding of HTML, HTTP, Server-side languages, XML, JavaScript.
- Good understanding and practical proficiency of XSS, XSRF, SQLi, and basic HTML5 attacks.
- Ability to read and understand PHP code will help, although not mandatory.
- Basic development skills required.

The eLearnSecurity WAPT course provides most of the above pre-requisites.

WHO SHOULD TAKE THIS COURSE?

The WAPTX course is primarily geared towards:

- Penetration Testers
- Web Developers
- IT Security professionals with a technical background

HOW AM I GOING TO LEARN THIS?

eLearnSecurity courses are very interactive, addictive, and presents content in such a way that it appeals to all learning styles. WAPTX comes with practical lessons and videos, so do not expect the outdated way of learning by just reading pages of theoretical methodologies. During this training course, you will have several guided labs that will provide you with relevant and hands-on practical application experience.

WILL I GET A CERTIFICATE?

Once you satisfy the requirements of the final practical certification test, you will be awarded an "eLearnSecurity Web Penetration Tester eXtreme" certificate and will hold the eWPTX certification.

ORGANIZATION OF CONTENTS

The WAPTX is a follow up of the WAPT course but at an "extreme" level. This course brings students into a new world of advanced exploitation techniques using real-world scenarios – all served with challenging and extremely hands-on laboratories in which to put the covered techniques into practice.

- Module 1: Encoding and Filtering
- Module 2: Evasion Basic
- Module 3: Cross-Site Scripting
- Module 4: XSS Filter Evasion and WAF Bypassing
- Module 5: Cross-Site Request Forgery
- Module 6: HTML 5
- Module 7: SQL Injections
- Module 8: SQLi Filter Evasion and WAF Bypassing
- Module 9: XML Attacks
- Module 10: Attacking Serialization
- Module 11: Server Side Attacks
- Module 12: Attacking Crypto
- Module 13: Attacking Authentication & SSO
- Module 14: Pentesting APIs & Cloud Applications
- Module 15: Attacking LDAP-based Implementations

MODULE 1: ENCODING AND FILTERING

The first module of this course is not just another module on encoding. It provides some esoteric encoding skills that will be helpful during the rest of the course. Understanding what kind of data encoding is used and how it works is fundamental and ensures that the tests are performed as intended, which is why this module starts with the basic concept of data encoding.

The Encoding and Filtering module is about filtering basics, starting from a brief introduction on how to deal with regular expression, to understanding how to detect, fingerprint, and evade web application firewalls. We conclude by analyzing the most common client-side defensive mechanism.

1. ENCODING AND FILTERING

- **1.1 Data Encoding Basics**
  - 1.1.1 Dissecting Encoding Types
    - 1.1.1.1 URL Encoding
    - 1.1.1.2 HTML Encoding
      - 1.1.1.2.1 Document Character Encoding
      - 1.1.1.2.2 Character References
    - 1.1.1.3 Base (36|64) Encoding
      - 1.1.1.3.1 Base 36
      - 1.1.1.3.2 Base 64
    - 1.1.1.4 Unicode Encoding
  - 1.1.2 Multiple (De|En)codings
- **1.2 Filtering Basics**
  - 1.2.1 Regular Expressions
    - 1.2.1.1 Metacharacters
    - 1.2.1.2 Shorthand Character Classes
    - 1.2.1.3 Non-printing Characters
    - 1.2.1.4 Unicode
  - 1.2.2 Web Application Firewall
    - 1.2.2.1 Simple Rules to Bypass WAFs
    - 1.2.2.2 WAF Detection and Fingerprinting
  - 1.2.3 Client-side Filters
    - 1.2.3.1 Browser Add-ons
    - 1.2.3.2 Native Browser Filters

MODULE 2: EVASION BASICS

The Evasion Basics module provides advanced coverage of most modern filter evasion techniques using different client-side and server-side languages. To ensure that you have a complete understanding of filters and encoding, the main evasion techniques that start from Base64 and lesser-known URI obfuscation techniques and concludes with JavaScript and PHP obfuscation techniques are introduced.

2. EVASION BASICS

- **2.1 Base64 Encoding Evasion**
  - 2.1.1 Cookie Stealer
- **2.2 URI Obfuscation Techniques**
  - 2.2.1 URL Shortening
    - 2.2.1.1 Bitly.com Short Link Info
    - 2.2.1.2 Other Services Short Link Info
    - 2.2.1.3 cURL Link Resolver
  - 2.2.2. URL Hostname Obfuscation
    - 2.2.2.1 URL Authority Obfuscation
- **2.3 JavaScript Obfuscation Techniques**
  - 2.3.1 JavaScript Encoding – Non-Alphanumeric
    - 2.3.1.1 String Casting
    - 2.3.1.2 Booleans
    - 2.3.1.3 Numbers
    - 2.3.1.4 String
      - 2.3.1.4.1 Generate 'alert' String
    - 2.3.1.5 JJencode
    - 2.3.1.6 AAencode
    - 2.3.17 JSFuck
  - 2.3.2 JavaScript Compressing
    - 2.3.2.1 Minifying
    - 2.3.2.2 Packing
- **2.4 PHP Obfuscation Techniques**
  - 2.4.1 Basic Language Reference
    - 2.4.1.1 Type Juggling
    - 2.4.1.2 Numerical Data Types
    - 2.4.1.3 String Data Types
    - 2.4.1.4 Array Data Types
    - 2.4.1.5 Variable Variables
  - 2.4.2 Non-alphanumeric Code
    - 2.4.2.1 Strings Generation
    - 2.4.2.2 Hackvector.co.uk

MODULE 3: CROSS-SITE SCRIPTING

Module three is entirely dedicated to cross-site scripting attacks. It starts with a brief recap of the different types of XSS and then introduces advanced attacking techniques and exotic XSS vectors. This module also covers how to use the most advanced tools available and exploit any XSS.

MODULE 3: CROSS-SITE SCRIPTING (cont.)

MODULE 4: XSS FILTER EVASION AND WAF BYPASSING

In this module, the student will learn about advanced filter evasion and WAF bypassing techniques. Starting from simple blacklisting filters, the student will go through different mechanisms to bypass common input sanitization techniques, browser filters, and much more. The student will not only find a number of well-known vectors but will also understand how to find new ones. At the end of this module, the student will be able to recognize the presence of WAF's and filters and implement effective bypassing techniques.

4. XSS FILTER EVASION AND WAF BYPASSING

- **4.1 Introduction**
- **4.2 Bypassing Blacklisting Filters**
  - 4.2.1 Injecting Script Code
    - 4.2.1.1 Bypassing Weak <script> Tag Banning
    - 4.2.1.2 ModSecurity > Script Tag Based XSS Vectors Rule
    - 4.2.1.3 Beyond <script> Tag…Using HTML Attributes
    - 4.2.1.4 Beyond <script> Tag…Using HTML Events
  - 4.2.2 Keyword Based Filter
    - 4.2.2.1 Character Escaping
      - 4.2.2.1.1 Unicode
      - 4.2.2.1.2 Decimal, Octal, Hexadecimal
    - 4.2.2.2 Constructing Strings
    - 4.2.2.3 Execution Sinks
    - 4.2.2.4 Pseudo-protocols
      - 4.2.2.4.1 Data
      - 4.2.2.4.2 Vbscript
- **4.3 Bypassing Sanitization**
  - 4.3.1 String Manipulations
    - 4.3.1.1 Removing HTML Tags
    - 4.3.1.2 Escaping Quotes
    - 4.3.1.3 Escape Parentheses
- **4.4 Bypassing Browser Filters**
  - 4.4.1 (Un)Filtered Scenarios - Injecting Inside HTML Tag
  - 4.4.2 (Un)Filtered Scenarios - Injecting Inside HTML Tag Attributes
  - 4.4.3 (Un)Filtered Scenarios - Injecting Inside SCRIPT Tag
  - 4.4.4 (Un)Filtered Scenarios - Injecting Inside Event Attributes
  - 4.4.5 (Un)Filtered Scenarios - DOM Based

MODULE 5: CROSS-SITE REQUEST FORGERY

This module is entirely dedicated to Cross-Site Request Forgery attacks. It starts from a brief recap about this vulnerability and then introduces the main Attack Techniques and Vectors in order to later introduce how to Exploit Weak Anti-CSRF Measures and to conclude Advanced Exploitation techniques.

MODULE 6: HTML5

Module six is entirely dedicated to HTML5 and its attack vectors. It starts with a recap of this language, analyzing the main features to focus our security research, and then dives deep into the main exploitation techniques and attack scenarios. Once the security concerns related to HTML5 features are analyzed, the student will learn about the most common security mechanisms developers use. These are critical in understanding how to leverage even more sophisticated attacks.

The module concludes with an analysis of the UI redressing attacks and an overview of related attack vectors introduced with HTML5.

6. HTML5

- **6.1 HTML5: Recap & More**
  - 6.1.1 Introduction
  - 6.1.2 Semantics
    - 6.1.2.1 Form Elements
    - 6.1.2.2 Media Elements
    - 6.1.2.3 Semantic/Structural Elements
    - 6.1.2.4 Attributes
  - 6.1.3 Offline & Storage
    - 6.1.3.1 Web Storage > Attack Scenario
      - 6.1.3.1.1 Session Hijacking
    - 6.1.3.2 Offline Web Application > Attack Scenario
  - 6.1.4 Device Access
    - 6.1.4.1 Geolocation > Attack Scenario
    - 6.1.4.2 Fullscreen Mode > Attack Scenario
      - 6.1.4.2.1 Phishing
  - 6.1.5 Performance, Integration & Connectivity
    - 6.1.5.1 Attack Scenarios
- **6.2 Exploiting HTML5**
  - 6.2.1 CORS Attack Scenario
    - 6.2.1.1 Universal Allow
      - 6.2.1.1.1 Allow by Wildcard Value*
      - 6.2.1.1.2 Allow by Server-Side
    - 6.2.1.2 Weak Access Control
      - 6.2.1.2.1 Check Origin Example
    - 6.2.1.3 Intranet Scanning
      - 6.2.1.3.1 JS-Recon

MODULE 6: HTML5 (cont.)

MODULE 7: SQL INJECTIONS

This module is entirely dedicated to SQL injection attacks, which recaps the main classification of exploitation techniques and then introduces advanced attack techniques on different DBMS's.

MODULE 7: SQL Injections (cont.)

- 7.3.1.3 OOB via DNS
  - 7.3.1.3.1 DNS Exfiltration Flow
  - 7.3.1.3.2 Provoking DNS Requests
    - MySQL (win)
    - MSSQL
    - Oracle
- 7.3.2 Exploiting Second-Order SQL Injection
  - 7.3.2.1 First-order Example
  - 7.3.2.2 Second-order Example
  - 7.3.2.3 Security Considerations
  - 7.3.2.4 Automation Considerations

MODULE 8: SQLi FILTER EVASION AND WAF BYPASSING

In this advanced module, the student will learn about advanced filter evasion and WAF bypassing techniques. These foundational skills will be necessary to understand and master further techniques. By the end of this module, the student will be able to recognize the presence of WAF's and filters and implement effective bypassing techniques.

MODULE 9: XML ATTACKS

Module nine is entirely dedicated to XML attacks, which starts with a recap of this language and then dives into the most modern attacks, such as XML Tag Injection, XXE, XEE, and XPath Injection. For each of them, basic and advanced exploitation techniques are analyzed. By the end of this module, the student will be able to pentest complex applications using XML.

9. XML ATTACKS

- **9.1 XML Attacks: Introduction, Recap & More**
  - 9.1.1 Introduction
  - 9.1.2 XML Attacks: Recap & More
    - 9.1.2.1 XML Document with Internal DTD
    - 9.1.2.2 XML Document with External DTD
    - 9.1.2.3 Entities
- **9.2 XML Tag Injection**
  - 9.2.1 Testing XML Injection - Single/Double Quotes
  - 9.2.2 Testing XML Injection - Ampersand
  - 9.2.3 Testing XML Injection - Angular parentheses
  - 9.2.4 Testing XML Injection - XSS with CDATA
- **9.3 XML eXternal Entity**
  - 9.3.1 Taxonomy
    - 9.3.1.1 External Entities: Private vs. Public
  - 9.3.2 XML eXternal Entity
    - 9.3.2.1 Resource Inclusion
    - 9.3.2.2 Resource Inclusion – Improved
      - Invalid resource to extract
      - CDATA Escape Using Parameter Entities
      - php://I/O Stream
  - 9.3.3 Bypassing Access Control
  - 9.3.4 Out-Of-Band Data Retrieval
    - OOB via HTTP
    - OOB via HTTP using XXEServe
- **9.4 XML Entity Expansion**
  - 9.4.1 Recursive Entity Expansion
    - 9.4.1.1 Billion Laugh Attack
  - 9.4.2 Generic Entity Expansion
    - 9.4.2.1 Quadratic Blowup Attack
  - 9.4.3 Remote Entity Expansion

MODULE 9: XML ATTACKS (cont.)

9.5 XPath Injection

9.5.1 XPath Recap

9.5.1.1 XPath 1.0 vs 2.0

- New Operations and Expressions on Sequences
  - Function on Strings
  - FOR Operator
  - Conditional Expression
  - Regular Expression
  - Assemble/Disassemble Strings
  - Data Types

9.5.2 Advanced XPath Exploitation

9.5.2.1 Blind Exploitation

- Error Based
- Boolean Based

9.5.2.2 OOB Exploitation

- HTTP Channel
- DNS Channel

MODULE 10: ATTACKING SERIALIZATION

In this module, you will learn about serialization and deserialization in Java, PHP, and .NET. We also present untypical serialization that you may come across during web application penetration testing. By the end of the module, you should have a better understanding of serialization mechanisms and how to find/exploit untrusted deserialization in common web technologies.

MODULE 11: SERVER-SIDE ATTACKS

In this module, you will come to understand how user-supplied input can sometimes be insecurely handled by back-end logic, as well as learn how to find and exploit server-side bugs. Specifically, during this module, you will learn how Server-Side Request Forgery, Server Side Include, Edge Side Include, Server Side Template Injection, and Expression Language Injection attacks work. Attacking XSLT engines is also covered. Note that the abovementioned attacks can have quite an impact on the overall security of an application since they can lead to not only sensitive information leakage but remote code execution as well.

MODULE 11: SERVER-SIDE ATTACKS (cont.)

MODULE 12: ATTACKING CRYPTO

This module will focus on identifying and attacking flawed or poorly constructed crypto implementations. Attacks such as Known Plaintext, Padding Oracle, Hash Length Extension, and Authorization bypass via .NET machine key will be covered.

MODULE 13: ATTACKING AUTHENTICATION & SSO

In module thirteen, you will have the opportunity to study advanced attacks against various Authentication and Single Sign On implementations. Before covering the attacks, you will dive into each implementation's internals, security shortcomings, and common misconfigurations. SAML, OAuth, JWT, and others will be covered.

13. ATTACKING AUTHENTICATION & SSO

- **13.1 Authentication in Web Apps**
- **13.2 Attacking JWT**
  - 13.2.1 JSON Web Tokens (JWT)
  - 13.2.2 JWT Security Facts
  - 13.2.3 JWT Attack Scenario 1
  - 13.2.4 JWT Attack Scenario 2
  - 13.2.5 JWT Attack Scenario 3
- **13.3 Attacking OAuth**
  - 13.3.1 OAuth
  - 13.3.2 Common OAuth Attacks
  - 13.3.3 OAuth Attack Scenario 2
  - 13.3.4 OAuth Attack Scenario 3
  - 13.3.5 OAuth Attack Scenario 4
- **13.4 Attacking SAML**
  - 13.4.1 Security Assertion Markup Language (SAML)
  - 13.4.2 SAML Security Considerations
  - 13.4.3 SAML Attack Scenario
- **13.5 Bypassing 2FA**
  - 13.5.1 2FA Bypasses
  - 13.5.2 2FA Bypass Scenario 1
  - 13.5.3 2FA Bypass Scenario 2

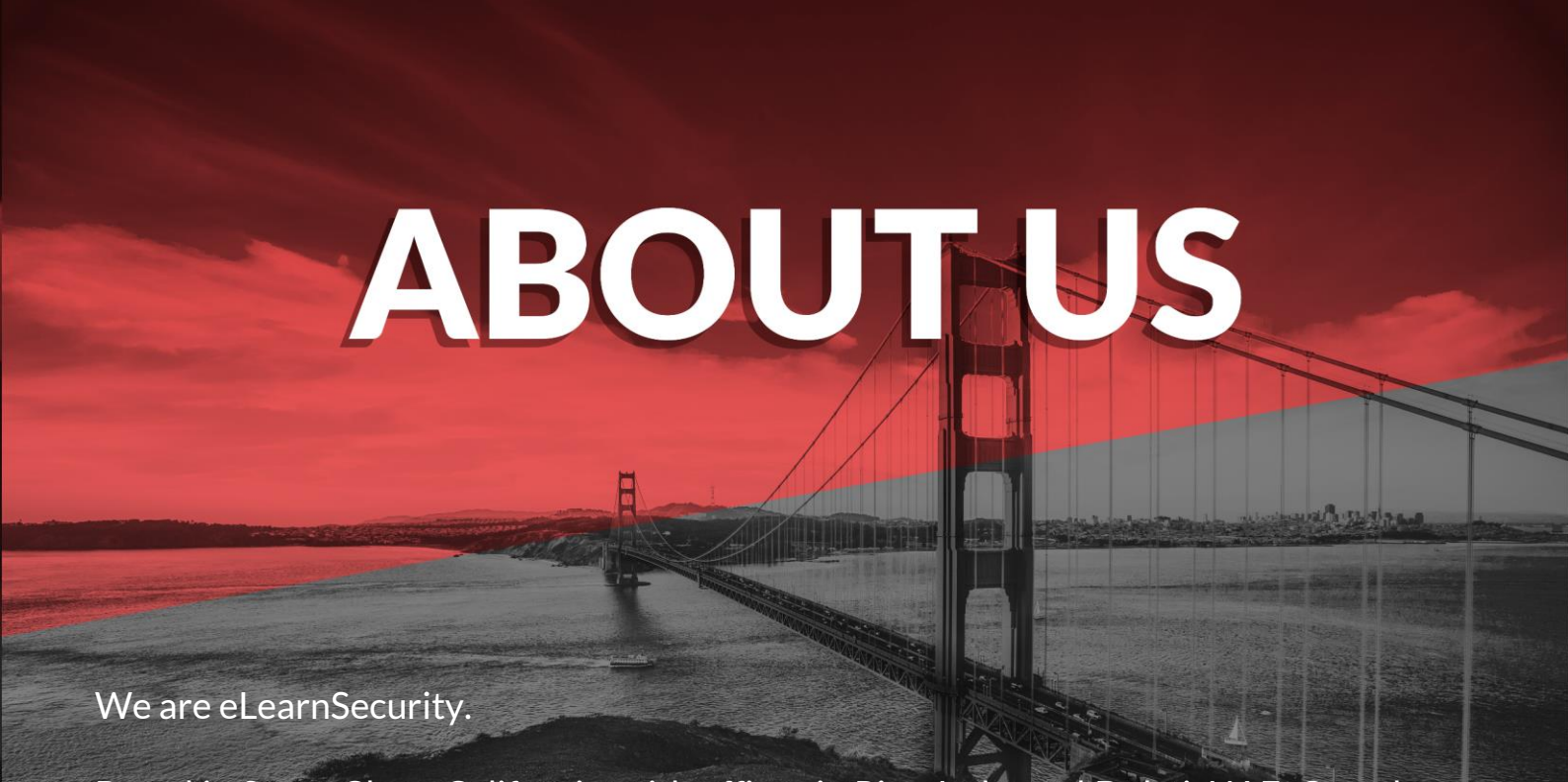
MODULE 14: PENTESTING APIS & CLOUD APPLICATIONS

APIs can be found in any IT aspect nowadays, from web and mobile applications all the way to IOT solutions and the cloud. It is of paramount importance for a penetration tester to be able to perform a thorough penetration test against an API. This module will cover in detail the most effective attacking tactics against APIs and Cloud-powered applications.

MODULE 15: ATTACKING LDAP-BASED IMPLEMENTATIONS

For numerous reasons, a web application can make use of LDAP (query objects from a directory database, authentication, management, etc.). In this module, you will learn how to exploit vulnerable LDAP-based implementations. Specifically, you will learn all about LDAP basics, LDAP injections, and LDAP manipulation/poisoning.

ABOUT US



We are eLearnSecurity.

Based in Santa Clara, California, with offices in Pisa, Italy, and Dubai, UAE, Caendra Inc. is a trusted source of IT security skills for IT professionals and corporations of all sizes. Caendra Inc. is the Silicon Valley-based company behind the eLearnSecurity brand.

eLearnSecurity has proven to be a leading innovator in the field of practical security training, with best of breed virtualization technology, in-house projects such as Coliseum Web Application Security Framework and Hera Network Security Lab, which has changed the way students learn and practice new skills.

Contact details:

www.elearnsecurity.com
contactus@elearnsecurity.com

2040 Martin Ave.
Santa Clara, CA, USA

Via Gian Battista Queirolo
Pisa, Italy

Apricot Tower, Dubai Silicon Oasis
Dubai, UAE